AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

3803 W. National Avenue, Apt. 3, West Milwaukee, WI 53215, a brown brick apartment building with light colored siding on the 2nd story of the building, including any storage area and vehicles associated with Apt. 3, as well as any person located within the residence. The building has brown trim and dark ornamental fencing along the second story deck of the building. "3803" is affixed to the brown trim of the second story deck on the north side of the building which faces National Avenue. The number "3" is affixed to the right side trim of the entrance door which faces northeast, on the National Avenue side of the building.

Case No. 19-MJ-1271

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. § 2252 (possessing and distributing child pornography)

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Amy Mentzel
Applicant's signature

FBI Special Agent Amy Mentzel
Printed Name and Title

Sworn to before me and signed in my presence:

Date: 6/24/19

William E. Duffin
Judge's signature

City and State: Milwaukee, Wisconsin

Hon. William E. Duffin, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT

I, Amy Mentzel, being first duly sworn, hereby depose and state as follows:

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since 2006. I am currently assigned to the FBI's Child Exploitation Task Force, Milwaukee Division. My duties include investigating criminal violations related to child exploitation and child pornography, including the receipt, possession, and distribution of child pornography, coercion and enticement of a minor to engage in sexual conduct, and the sexual exploitation and sexual abuse of minors, to include commercial sexual exploitation. I have experience investigating criminal violations related to state and federal child pornography laws, including executing search warrants and conducting interviews of individuals participating in the trading and manufacturing of child pornography. I have also received training in the investigation and enforcement of federal child pornography laws in which computers and other digital media are used as a means for receiving, transmitting, and storing child pornography.

2. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, as well as through information provided to me by other law enforcement officers whom I consider to be truthful and reliable. Some of the information was provided in response to administrative subpoenas and I believe this information to also be reliable.

3. Based upon the information described below, I submit that probable cause exists to believe a person accessing the internet at 3803 W. National Avenue, Apartment 3, West Milwaukee, Wisconsin (Subject Premises), more particularly described in Attachment A, has committed the crimes of possessing and distributing child pornography, in violation of 18 U.S.C. § 2252 and evidence relating to this crime, more particularly described in Attachment B, can be found at the subject premises.

4. Because this affidavit is being submitted for the limited purpose of establishing probable cause for the requested warrant, it does not set forth all of my knowledge about this matter.

DEFINITIONS

5. The following definitions apply to the affidavit and Attachment B to this affidavit:

a. "Camera" means a device used for recording visual images in the form of photographs, film, or video signals. Digital cameras record and store images in a digital format, which can include Digital8, MiniDV, DVD, a hard drive, or solid-state flash memory.

b. "Cellular telephone" or "cell phone" means a hand held wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications,

wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geolocation information indicating where the cell phone was at particular times.

c. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but are not, in and of themselves, legally obscene or do not necessarily depict minors in sexually explicit conduct.

d. "Child Pornography" is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. "Cloud" or "cloud storage" is a mechanism in which files can be saved to an off-site storage system maintained by a third party – i.e., files are saved to a remote database instated of the (user's) computer's hard drive. The internet provides the connection between the user's computer and the database for saving and retrieving files.

f. "Computer" is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

g. "Computer Server" or "Server," is a computer attached to a dedicated network and serves many users. A web server, for example, is a computer that hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system (DNS) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

h. "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts used to

restrict access to computer hardware (including, but not limited to, physical keys and locks).

i. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

j. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

k. "Computer passwords, pass phrases and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass phrase (a string of alphanumeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys that perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

l. "Electronic storage devices" includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information

(e.g., external hard drives and USB "thumb drives"). Many of these devices also permit users to communicate electronic information through the Internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

m. "Hash Value" refers to the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data. A hash value can be thought of as a "digital fingerprint" for data. If the data is changed, even slightly (like the addition or deletion of a comma or a period), the hash value changes. Therefore, if a file such as a digital photo is a hash value match to a known file, it means the digital photo is an exact copy of the known file.

n. "Internet Service Providers" (ISPs) are commercial organizations in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a

telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

o. An "Internet Protocol address" (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to the electronic storage device may be directed properly from its source to its destination. Most ISPs control a range of IP addresses. Some computers have static – that is, long-term – IP addresses, while other computers have dynamic – that is, frequently changed – IP addresses.

p. "Media Access Control" (MAC) address means a hardware identification number that uniquely identifies each device on a network. The equipment connecting a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter. This MAC address is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

q. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

r. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

s. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

t. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use URLs on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

u. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

ELECTRONIC STORAGE DEVICES AND FORENSIC ANALYSIS

6. I have consulted with laypersons and law enforcement officers with specialized knowledge and training in computers, networks, and Internet communications. In particular, I consulted with FBI Computer Analysis Response Team Forensic Examiner (CART-FE) Kerry Kolecheck, who has received specialized training as a forensic computer, cellular telephone, and other electronic storage device examiner. CART-FE Kolecheck has been a forensic computer examiner with the FBI since 2011. CART-FE Kolecheck has participated in the execution of numerous search warrants and search and seizure operations. CART-FE Kolecheck has informed me that to properly retrieve and analyze electronically stored (computer) data, and to insure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the electronic storage devices. To affect such accuracy and completeness, it may also be necessary to analyze not only the electronic storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the device computer and software. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the proposed search location, in whatever form they are found. One form in which the records might be

found is stored on a computer's hard drive, other storage media, or within a hand-held electronic device such as a cellular telephone or a tablet device (e.g., an iPad device). Some of this electronic information, as explained below, might take a meaningful form only upon forensic analysis.

7. Based on my knowledge, training, and experience, and after having consulted with CART-FE Kolecheck, I know computer and other electronic device hardware, peripheral devices, software, electronic files, and passwords may be important to a criminal investigation in three distinct and important respects:

a. The objects themselves may be instrumentalities used to commit the crime;

b. The objects may have been used to collect and store information about crimes (in the form of electronic data);

c. The objects may be contraband or fruits of the crime.

8. I submit that if a computer or other electronic storage device is found on the premises, there is probable cause to believe information will be saved to that electronic storage device, for the following reasons:

a. Based on my knowledge, training, and experience, I know electronic storage device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person deletes a file on an electronic storage

device, the data contained in the file does not actually disappear; rather, the data remains on the storage medium until it is overwritten by new data. Deleted files, or remnants of deleted files, may reside in free space or slack space, that is, in space on the storage medium that is not currently being used by an active file for long periods before they are overwritten. In addition, if the electronic storage device uses an operating system (in the case, for example, of a computer, cellular telephone or tablet device) the device may also contain a record of deleted data in a swap or recovery file.

b. Wholly apart from user-generated files, electronic storage device storage media, in particular, computers' internal hard drives, contain electronic evidence of how the device was used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, and file system data structures. Electronic storage device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Files viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or cache. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

9. As further described in Attachment B, this application seeks permission to locate not only electronic storage device files that might serve as direct evidence of the

crimes described on the warrant, but also for evidence establishing how electronic storage devices were used, the purpose of their use, who used them, and when.

10. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), electronic storage device storage media can contain other forms of electronic evidence as described below:

a. Data on the storage medium not currently associated with any file can provide evidence of a file once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic storage device was in use. Electronic storage device file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within an electronic storage device and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within an electronic storage device (e.g., registry information,

communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic storage device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic storage device was remotely accessed, thus inculpating or exculpating the electronic storage device owner. Further, electronic storage device activity can indicate how and when the electronic storage device was accessed or used. For example, as described herein, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within an electronic storage device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or cellular telephone may show a particular location and have geolocation information incorporated into its file data. Such file data typically contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera). The geographic and

timeline information described herein may either inculpate or exculpate the electronic storage device user. Last, information stored within an electronic storage device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the electronic storage device may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the electronic storage device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on an electronic storage device is relevant to the investigation may depend on other information stored on the electronic storage device and the application of knowledge about how an electronic storage device works. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

d. Further, in finding evidence of how an electronic storage device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience it is possible malicious software can be installed on a computer, often without the computer user's knowledge, which can allow the

computer to be used by others, sometimes without the knowledge of the computer owner.

11. I know from my training and experience, as well as from information found in publicly available materials, that some electronic devices offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") which is read via an integrated biometric device in lieu of a numeric or alphanumeric passcode or password. This feature often referred to as a fingerprint scanner, a fingerprint reader, or for Apple devices, Touch ID.

12. If a user enables the fingerprint scanner on a given device, he or she can register multiple fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's fingerprint scanner, which can be found in different locations on the device depending on the manufacturer. In my training and experience, users of devices that offer fingerprint scanners often enable it because it is considered a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

13. In some circumstances, a fingerprint cannot be used to unlock a device that has its fingerprint scanner enabled, and a passcode or password must be used instead. Thus, in the event law enforcement encounters a locked device, the opportunity to unlock the device via the fingerprint scanner exists only for a short time.

The fingerprint scanner also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) too many unsuccessful attempts to unlock the device via the fingerprint scanner are made.

14. If fingerprint scanner enabled devices are found during a search of the premises, the passcode or password that would unlock such devices are presently unknown to law enforcement. Thus, it will likely be necessary to press the fingers of the user(s) of any device(s) found during the search of the premises to the device's fingerprint scanner in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the device(s) via fingerprint scanner with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

15. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via the fingerprint scanner, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Further, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will

likely be necessary for law enforcement to have the ability to require any occupant of the premises to press their finger(s) against the fingerprint scanner of the locked device(s) found during the search of the premises in order to attempt to identify the device's user(s) and unlock the device(s) via the fingerprint scanner.

16. Based upon my knowledge, training and experience, and after having consulted with CART-FE Kolecheck, I know a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some electronic storage device equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files easily viewed on site. Analyzing evidence of how an electronic storage device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular

files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Technical requirements. Electronic storage devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of electronic storage device hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

17. In light of these concerns, I hereby request permission to seize the electronic storage devices, associated storage media, and associated peripherals believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude it would be impractical to search the hardware, media, or peripherals on-site for this evidence.

18. I know when an individual uses a computer to commit crimes involving child pornography, the individual's computer will generally serve both as an

instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic storage device is an instrumentality of the crime because it is used as a means of committing the criminal offense. From my training and experience, I believe an electronic storage device used to commit a crime of this type may contain evidence of how the electronic storage device was used, data sent or received, notes as to how the criminal conduct was achieved, records of Internet discussions about the crime, and other records that indicate the nature of the offense.

19. "Dropbox" refers to an online storage medium on the internet accessed from a computer or electronic storage device. As an example, online storage mediums such as Dropbox make it possible for the user to have access to saved files without the requirement of storing said files on their own computer or other electronic storage device. Dropbox is an "offsite" storage medium for data viewed at any time from any device capable of accessing the internet. Users can store their files on Dropbox and avoid having the files appear on their computer. Anyone searching an individual's computer that utilizes Dropbox would not be able to view these files if the user opted only to store them at an offsite such as Dropbox. These are often viewed as advantageous for collectors of child pornography in that they can enjoy an added level of anonymity and security.

20. Dropbox provides a variety of online services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to

provide basic personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

21. When the subscriber transfers a file to a Dropbox account, it is initiated at the user's computer, transferred via the Internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.

22. Online storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices accessed the account.

23. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

DETAILS OF THE INVESTIGATION

24. On March 19, 2019, I received reports from the National Center For Missing and Exploited Children (NCMEC) pertaining to multiple Dropbox CyberTips they had received. A NCMEC Cybertip is a mechanism for the public or an electronic service provider to report possible online exploitation of children. On October 3, 2018, Dropbox submitted a CyberTip to NCMEC that user, "Laural Raines" utilizing email account lauralraines@gmail.com, had uploaded 141 videos containing child pornography. According to the NCMEC report, a NCMEC analyst reviewed the videos provided by Dropbox and determined that the videos did contain child pornography material.

25. On November 2, 2018, NCMEC analyst Breelle Hunter, served Dropbox with an administrative subpoena for full subscriber information for the account. On November 8, 2018, Dropbox responded with the following information:

Name: Laural Raines
Email: lauralraines@gmail.com
User ID: 1027006608
Current Account Status: Disabled
Subscription Status: Free

Mobile Information

TIMESTAMP (UTC) | IP | MODEL | CARRIER |
+----------+----------
| 2018-08-20 04:19:16 GMT | 2607:fb90:a33f:d287:3bca:5823:163e:bd3 | Z982 | MetroPCS |
| 2018-09-30 21:45:50 GMT | 2605:a000:b141:3400:a176:3fac:272a:f87a | Z982 | MetroPCS |

26. On November 2, 2018, NCMEC analyst Breelle Hunter, also served Google with an administrative subpoena for subscriber information pertaining to the lauralraines@gmail.com email address identified in the Dropbox subscriber information. On November 8, 2018, Google responded with the following information:

Name: Laural Raines
Email: lauralraines@gmail.com
Services: Android, Gmail, Google Calender, Google Keep, Location History, Minutemaid, Web & App Activity, YouTube
Created on: 2018/04/13-02:32:54-UTC
Terms of Service IP: 2607:fb90:263:685e:67d8:f96b:6b7c:2994, on 2018/04/13-02:32:54-UTC
SMS: +14144122487 [US]
Google Account ID: 417602629805
Last Logins: 2018/09/02-20:20:18-UTC, 2018/07/01-00:40:05-UTC, 2018/06/17-22:23:15-UTC

27. On November 13, 2018, NCMEC analyst Breelle Hunter served T-Mobile with an administrative subpoena for subscriber information pertaining to telephone number 414-412-2487. This telephone number was identified in the aforementioned Google subscriber information as a number listed by the subscriber for "SMS" or Short Message Service (text messaging). T-Mobile provided the following subscriber information:

Customer Name: DENNIS CZYSZ
Subscriber Name: DENNIS CZYSZ
Service Address: 822 N. 24th St Milwaukee WI 53233-1502

Billing Address: 822 N. 24th St Milwaukee WI 53233-1502
Email Address:
Start Time: Dec 15, 2017 08:00:00 (UTC)
End Time: Jan 01, 0001 08:00:00 (UTC)

28. On November 13, 2018, NCMEC analyst Breelle Hunter also served Charter Communications with an administrative subpoena pertaining to IP address 2605:a000:b141:3400:a176:3fac:272a:f87a, on September 30, 2018 at 21:45:50 GMT. This was the most recent IP address identified in the Dropbox subpoena subscriber information. Charter Communications provided the following subscriber information for the IP address:

Subscriber Name: dennis czysz
Subscriber Address: 3657 E. Layton Ave,7, Apt.7, Cudahy, WI 53110-1410
User Name or Features: dennis.czysz@yahoo.com
Phone number: (414) 412-2487
Account Number: 32968702
MAC: 08952a622888
IP Lease Information Lease Start: 10/25/2017 3:56:57 PM Through 11/6/2018 8:19:29 PM
Length of Service: 10/25/2017-11/1/2018
Types of Service: Data, Phone, Video
Method of Payment: Visa x4245

29. Analysts at NCMEC then queried the NCMEC database using the identifiers obtained from the subpoena results. NMCEC located CyberTipline Report #7917796 from January 8, 2016 by Dropbox. Dropbox indicated that a user with the email address, dennis.czysz@yahoo.com, with a screen name, Jacob Moreno, uploaded 40 videos depicting child pornography to the user's Dropbox account. The Cybertip indicated that a NCMEC analyst reviewed some of the videos from the Dropbox

account and found them to be consistent with child pornography. There did not appear to be any additional investigative steps taken regarding the 2016 CyberTipline Report.

30. Analysts at NCMEC conducted criminal history checks for Czysz through the National Crime Information Center (NCIC) and learned that Czysz was a registered sex offender. Czysz was convicted of Exposing a Child to Harmful Materials in June 2000 and Possession of Child Pornography in 2005. Czysz's address listed on the Wisconsin Department of Corrections Sex Offender Registry was 3803 W. National Avenue, Apartment 3, Milwaukee, Wisconsin, 53215. NCMEC analysts also conducted public database searches and found that Czysz's listed address since December 2018 was 3803 W. National Avenue, Apartment 3, Milwaukee, Wisconsin. This address is located within the city limits of West Milwaukee, Wisconsin.

31. On June 19, 2019, Corrections Program Specialist, Monica Lukach, of the Wisconsin Department of Corrections (DOC), provided information that Czysz completed a letter on November 8, 2018, indicating his current address was 3803 W. National Avenue, Apartment 3, Milwaukee, Wisconsin 53215. I reviewed the letter and Czysz also indicated his telephone number was 414-412-2487. I know this telephone number to be the same number listed in the Google subscriber information for the lauralraines@gmail.com account, which was the email account Dropbox identified as uploading 141 child pornography videos in 2018. I conducted database checks of the name Laural Raines on June 18, 2019, and was unable to find any adult by that name who is associated with Czysz. Czysz also indicated in the letter to the DOC that he utilized the internet at his residence and his email account is dennis.czysz@yahoo.com.

This email account was identified by Dropbox in 2016, as the subscriber email for the account using the screen name "Jacob Moreno." The user of this account uploaded 40 videos depicting child pornography.

32. On April 17th and 24th, 2019, and again on May30th, 2019, agents, including Special Agent Gregory Zack, conducted surveillance at 3803 W. National Avenue, Apartment 3, West Milwaukee, Wisconsin. Surveillance agents observed Czysz entering and leaving the Subject Premises. On April 24th, 2019, Czysz was observed gaining access to the Subject Premises with a key. On June 19, 2019, Czysz was observed again by surveillance agents entering the Subject Premises.

33. In addition to the March 19, 2019 Cybertip information, I also received a flash drive from NCMEC containing the child pornography videos that were provided to NCMEC by Dropbox from both the 2016 and 2018 Cybertips. There were 141 videos containing child pornography provided from the 2018 "Laural Raines" Dropbox account.

34. I reviewed video, "ee306903-24fe-4817-9697-9dd4c55cdcb3.mp4," provided by Dropbox from the 2018 "Laural Raines" Cybertip. The video depicts a young female between the ages of 5 and 8 lying on her back completely nude. A male child of indeterminate age is engaging in penis to vagina intercourse with the female child. Simultaneously, an adult male is engaging in penis to mouth sexual intercourse with the female child. Neither the face of the man, nor the male child are visible in the video. The video then transitions to an adult male engaging in penis to anus sexual intercourse with the same female child. The video is approximately two minutes long.

35. I reviewed a video entitled, "Video Jan 26, 22 58 27.mp4," provided by Dropbox from the 2018 "Laural Raines" Cybertip. The video depicts a young female between 6 and 9 lying on her back and nude from the waist down. The girl's legs are up in the air and her face is seen very briefly. The camera zooms in on her vagina and a male voice states, "Let me look inside you." He instructs the girl to put her legs up higher and then tells the girl to "stay still." As the camera gets extremely close, the inside of the girl's vagina is visualized and the male states, "Nice and opened up, no more skin in the way." An adult male finger is then placed inside the girl's vagina, and the male voice states, "That's so tight, I'm touching your cervix right now." The next scene depicts penis to vagina sexual intercourse of an adult penis and a child's vagina. The same male voice states, "Spread your pussy a little with your fingers; pull it apart. That's it. Yep keep it stretched out like that. Pull it open so they can see. Pull it open." The video lasts approximately two minutes.

36. I reviewed video "3d9b51f2-9a94-450f-a316-cdaf2e311e1b.mp4," provided by Dropbox from the 2018 "Laural Raines" Cybertip. The video depicts a female child between the ages of 5 and 8, sitting on a chair. The video is being filmed from the side of the chair and the child turns her head to look at the camera and appears to be talking to the person who is recording the video. There is no sound in the video and the child is wearing a pink flowered top. An adult male then approaches the child from the front and places his penis in front of her face. The child begins stroking the penis with both hands and opens her mouth while looking at the camera. The child then abruptly turns her head to the opposite side of the camera places her hands over her mouth. The male

places his hand on the child's head and forcibly turns her head back to his penis as the child breathes deeply. He then places the tip of his penis in the child's mouth as the child looks toward the camera. The video lasts approximately 23 seconds.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO RECEIVE AND POSSESS CHILD PORNOGRAPHY

37. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who receive and possess images of child pornography:

a. Individuals who receive and possess child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals who receive and possess child pornography may collect sexually explicit or suggestive materials, in a variety of media, including electronically, or through photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who receive and possess child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

d. Individuals who receive and possess child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Individuals who receive and possess child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND ON ELECTRONIC STORAGE DEVICES AND CHILD PORNOGRAPHY

38. Computers, cellular telephones, and other electronic storage devices (collectively electronic storage devices) have dramatically changed the way in which individuals interested in child pornography interact with each other. Electronic storage

devices basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

39. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a device by simply connecting the camera to the electronic storage device. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards can store terabytes of data, which provides enough space to store thousands of high-resolution photographs. Video recorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the video recorder to a computer. Many electronic storage devices (e.g., computers, cellular telephones, and tablets), have cameras built into the device which allows users to create and store still and video images on the device. Moreover, if the device has Internet connectivity, users can distribute still and video images from the device.

40. Internet-enabled electronic storage devices can connect to other Internet-enabled devices. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child

pornography can be transferred via e-mail or through file transfer protocols (FTPs) to anyone with access to an Internet-enabled electronic storage device. Because of the proliferation of commercial services that provide e-mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, electronic storage devices are the preferred method of distribution and receipt of child pornographic materials.

41. Electronic storage devices are the ideal repository for child pornography. The amount of information an electronic storage device can hold has grown exponentially over the last decade. Electronic storage devices can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on a computer or other electronic storage device. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Many electronic storage devices can easily be concealed and carried on an individual's person.

42. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

43. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and

Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any internet-enabled electronic storage device. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's electronic storage device in most cases.

44. As is the case with most digital technology, communications by way of electronic storage device can be saved or stored on the device. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, an electronic storage device user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

45. Based on my knowledge, training, and experience, I know electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data

contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

CONCLUSION

46. I submit this affidavit supports probable cause for a warrant to search the premises described in Attachment A and seize the items described in Attachment B.

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED ("PREMISES")

The location known as 3803 W. National Avenue, Apartment 3, West Milwaukee, Wisconsin 53215, a brown brick apartment building with light colored siding on the 2nd story of the building. The building has brown trim and dark ornamental fencing along the second story deck of the building. "3803" is affixed to the brown trim of the second story deck on the north side of the building which faces National Avenue. The number "3" is affixed to the right side trim of the entrance door which faces northeast, on the National Avenue side of the building.

The Premises to be searched also includes any storage area and vehicles associated with Apartment 3, as well as any persons located within the residence.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Cell phones, computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography, display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. 2256(2).
4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C 2256(8), visual depictions of minors

engaged in sexually explicit conduct as defined in 18 U.S.C 2256(2), or child erotica.

5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of any device by use of the computer or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C 2256(2).
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256(2).
7. Any and all notes, documents, records or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256(2).
8. Any and all notes, documents, records, or correspondence, in an format or medium (including, but not limited to, envelopes, letters, papers, e-mail

messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all cameras, film, videotapes or other photographic equipment.

13. Any and all visual depictions of minors.

14. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of name so r lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256(2).

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256(2).

16. For any electronic storage device, computer hard drive, electronic device, or other physical object which electronic information can be recorded (hereinafter, "electronic storage device") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

    a. Evidence of who used, owned, or controlled the electronic storage device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email

contacts, "chat," instant messaging logs, photographs, and correspondence;

b. Evidence of software that would allow others to control the electronic storage device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. Evidence of the lack of such malicious software;

d. Evidence indicating how and when the electronic storage device was accessed or used to determine the chronological context of electronic storage device access, use, and events relating to crime under investigation;

e. Evidence indicating the electronic storage device user's location and state of mind as it relates to the crime under investigation;

f. Evidence of the attachment to the electronic storage device of other storage devices or similar containers for electronic evidence;

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage device;

h. Evidence of the times the electronic storage device was used;

i. Passwords, encryption keys, and other access devices that may be necessary to access the electronic storage device;

j. Documentation and manuals that may be necessary to access the electronic storage device or to conduct a forensic examination of the electronic storage device;

k. Contextual information necessary to understand the evidence described in this attachment.

17. Records and things evidencing communication with the internet, including:

a. Routers, modems, and network equipment used to connect electronic storage devices to the Internet;

b. Records of Internet Protocol addresses used;

c. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage device or electronic storage; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the

premises to the Touch ID sensor of Apple brand device(s), such as an iPhone or iPad, found at the premises for purpose of attempting to unlock the devices via Touch ID in order to search the contents as authorized by this warrant.